Testimony of

The Computing Technology Industry Association (CompTIA)

Roger J. Cochetti

Group Director-U.S. Public Policy

Before the House Small Business Committee

Subcommittee on Finance and Tax

On

"Data Security: Small Business Perspectives"
Wednesday, June 6, 2007

Good morning, Chairwoman Bean, Ranking Member Heller, and distinguished members of the Subcommittee. My name is Roger Cochetti. I am Group Director for U.S. Public Policy of the Computing Technology Industry Association (CompTIA) and I am here today on behalf of our 20,000 member companies.

Madam Chairwoman, I want to thank you and the Members of your Subcommittee for holding this important hearing on the state of small business data security. Data security breaches, often caused by opportunistic cyber criminals and frequently enabled by human errors, can be prevented by, in most cases, using the right combination of training, technology tools, procedures, and public/private sector collaboration. We believe that your efforts to focus public attention on the factors that affect data security and small business will help American small businesses more ably address, thwart and remediate data security threats.

CompTIA: Association Overview and Role in IT Security.

The Computing Technology Industry Association represents the business interests of the information (IT) industry. For 25 years, CompTIA has provided research, networking and partnering opportunities to its 20,000, mostly-American, member companies. While we represent nearly every major computer hardware manufacturer and software publisher, nearly 75% of our membership is comprised of American Value Added Resellers, or VARs. These small, system integrators set up and maintain computer systems and networks for small businesses. An estimated 32,000 American VARs sell some $43 billion dollars worth of computer hardware, software and services -- mostly to the small businesses that drive the American economy. This means that around one-third of the computer hardware and software sold in the U.S. today is sold by VARs; again mostly to small businesses. VARs are the front line in protecting critical data from cyber criminals. We particularly appreciate the opportunity to testify before this Subcommittee, because for our VAR members, data security is not a theoretical concern: It is what they must build into the services that they provide to their clients.

As this Subcommittee knows, small business is the backbone of the American economy. Some 23 million small businesses employ over half of the private sector workforce and are a vital source of the entrepreneurship, creativity and innovation that keeps our economy globally competitive. They are responsible for over half of our GDP, and their share is growing. Moreover, Americans depend upon small business for virtually every aspect of their daily lives. So, as a nation, we are dependent upon the health of the small business sector. And small business, in turn, relies on our members for its information technology services.

VARs service just about every small business in America. Your dentist, travel agent, local retailer, or dry cleaner almost certainly contracts with their local VAR to install, maintain and service their IT needs. For example, the local area network in your dentist's office is most likely not installed or maintained by the dentist. Nor is it installed and

maintained by a multinational computer hardware or software company. This work is almost certainly performed by a local VAR.

While CompTIA is distinct in its representation of Americas tens of thousands of VARs, I wish to also emphasize that we represent most of America's principal computer hardware, software, and services companies. In addition to representing the interests of our members through our headquarters in Chicago, and our public policy offices in Washington, Brussels, Hong Kong and Sao Paulo, CompTIA works to provide global policy leadership for the IT industry, and nowhere are we more active than in the area of cyber security policy.

Finally Madam Chairwoman, for most people who work with computer technology, CompTIA is probably best known for the non-policy-related services that it provides to advance industry growth: standards, professional certifications, industry education and business solutions.

In order to most efficiently serve the industry and our members, CompTIA has developed specialized initiatives and programs dedicated to major areas within the IT industry. Some of the services that we offer that are relevant to this hearing include:

· Professional Certifications for IT Workers

CompTIA offers 12, vendor-neutral professional certifications that test and validate a variety of baseline technical and professional IT skills. CompTIA A+, Network+, CDIA+, PDI+, Server+, Linux+, IT Project+, Convergence+, CTT+, DHTI+ (Home Technology Integrator), RFID+, and Security+ certifications provide credibility, recognition of achievement and quality assurance for employers and employees alike.

Today, almost one million CompTIA certificates have been issued; mostly to American IT professionals. And these CompTIA 'alumni' are an important source of insight and input for us as we address issues like data security and cyber security.

Importantly for this hearing, we have developed the Security+ professional certification. Security+ is the industry standard for validating an IT professional's abilities in the areas critical to data security including infrastructure security, communications security, operational security, and basic cryptography. For the business community, Security+ certified employees and contractors means a reduced risk of network breaches and an improved ability to prevent and mitigate cyber crime. To date, around 35,000 people have taken our Security+ certification exam, making it the most important cyber security professional certification in the United States.

· Helping the IT Industry Understand Privacy Regulations

CompTIA provides a formal structure and method for managers in the IT industry to communicate and resolve industry issues such as standard terminology in warranties and how to address new and challenging regulations that IT companies collectively face. We have launched a series of parallel efforts to help the industry understand the complexities, and implications for IT integrators, of such recent Federal regulations in the area of consumer privacy as those resulting from Graham-Leach-Bliley (GLB) and the Health Insurance Portability and Accountability Act (HIPAA). Threats to consumer privacy under the practices regulated by these laws and regulations very often result from cyber crime. This is as true for small businesses as it is for large companies.

· Educating VARs and Other Small IT Companies on Cyber Crime

With support from Federal and State officials and many of our larger member companies, in 2005 we launched a series of modest educational outreach programs for VARs on the problems and issues raised by cyber security. These new programs aim to reach out to the thousands of small IT businesses that make up the bulk of our membership and help them better understand what the Federal and State governments and large corporations are doing in this area and explain how they can get more involved.

· Public Policy

CompTIA's public policy program addresses the policy and regulatory concerns of the IT community at the federal, state and international levels. We do this by educating our members about developments in the policy process and encouraging them to get more engaged and by advocating policy solutions that make sense for the nation and for the IT industry.

Given the importance of small business to the U.S. economy and the importance of VARs as the IT enablers of small business, it is somewhat surprising and disappointing to us that cyber crime and data security concerns of small businesses have not received greater attention. At the federal level, several important but modest efforts have been launched aimed at educating small business about the basic issues in IT security; and we are pleased to say that we have been involved in nearly all of them. As I will explain later, we believe that much more needs to be done, however.

The State of Small Business IT Security.

Beginning in 2002, CompTIA has commissioned an annual IT security benchmark study entitled "Committing to Security – A CompTIA Analysis of IT Security and the Workforce." This study is a cross-sector analysis of the state of IT security as well as an examination of the root cause of most IT security breaches.

The benchmark study surveys professionals across a myriad of industries who are asked to answer pressing questions about the dynamic landscape of IT security. Our study also provides insights into IT security practices and highlights security challenges confronted by organizations of varying sizes and sectors. Approximately 28% of the respondents are small businesses with annual revenues below $10 million, and another 20% are businesses with annual revenues from $10 million to less than $100 million.

To briefly summarize, CompTIA's IT Security Study reveals that the IT security landscape has changed significantly, along with the rapidly changing technology used across industries. As we all know, the opportunities of Internet communications and commerce in the global marketplace have been exploited by some with malicious intent. Although procedures and cyber security technology tools have become increasingly more advanced in their ability to detect security threats to networks, applications and operating systems, malicious hackers are often sophisticated enough to find gaps in procedures, failures to comply with procedures, or to reverse-engineer technology tools. Even the most sophisticated cyber security procedures or technology tools, however, cannot replace the need for IT security training and certification in the workplace.

Most non-technology based organizations are slower to adopt new procedures, cyber security tools and slower to implement cyber security training and certification for employees. Employees with cyber security responsibilities, but without adequate training and certification, can easily underestimate a threat of security breaches to their organization. Other decision-makers, including small business managers, lack the empirical support to rationalize the needed investment for IT security.

Overall, CompTIA's Cyber Security Study reveals a large discrepancy between the IT security that organizations say they need and the level of education and prevention occurring within these organizations. In 2006, the fifth annual CompTIA Study on IT Security and the Workforce found that nearly 34% of organizations experienced an IT security breach within the last year. While that number has declined from 2005, the survey found a higher level of severity in the breaches that did occur. On a scale of 1 to 10, with 10 being most severe, the average breach in 2005 was a 2.3; in 2006 that number grew to a 4.8.

More specifically, while the study found that over 32% of respondents reported facing data theft issues, up dramatically from 19.8% in 2004, and 50% of respondents reported that data theft threats had increased over the past year, it also found that organizations, including small businesses, may not be taking all the steps necessary to protect

themselves. 61% of small businesses do not have a written IT security policy in place, and small businesses are less likely to report a security breach.

Overwhelmingly, 81% of responding organizations believe that major security breaches have been reduced as a result of IT security training and certification. The positive effect of training and certification is most often described in terms of improved potential risk identification, increased awareness, improved security measures and an ability to respond more rapidly to problems. The lack of written IT security policies for more than 60% of the responding small businesses fosters gaps in security knowledge, especially among end-users. Even in organizations with written security policies in place, enforcement of security policies continues to be a problem.

Combating Data Security Breaches: Training and Technology Used to Fight Cyber Criminals and Prevent Human Errors.

Madam Charwoman, we have found that data security breaches at businesses generally occur as a result of one or more of the following: Low-tech crime; high-tech (or cyber) crime, and human error. Low tech crimes are represented by more traditional criminal activity, such as physically stealing a computer from an office, home or car, or a company's employee stealing information or hardware from the workplace. VARs use technology tools such as password protection and encryption to help prevent criminal access to data if it has been stolen using low-tech methods, and can use low-tech physical tools, such as computer locks and lockers, to prevent physical theft. Obviously, CompTIA's members do not commonly address the physical security concerns that are the first line of defense against low-tech crime. But we are quite concerned with the physical aspects of IT security and most of our members work with their customers to improve basic physical computer security.

Cyber crime, as distinct from low-tech crime, often does not involve the physical removal of computer hardware from a business. A cyber criminal doesn't need to physically go

inside a business to steal data. Criminals can remotely enter computers and steal data using malicious software programs distributed via email, email attachments and internet downloads. Additionally, data could be accessed by cyber criminals entering a business' wireless network using a laptop in the vicinity of the business. Our members help their customers by using procedures and technology tools both to prevent malicious programs from entering a businesses network and to prevent unauthorized entry into the network. For procedures and technology to be effective, both the technology integrator and the end user need to thoroughly understand the procedures and the technology tools themselves. To that end, our members can also provide basic employee training for a customer's employees on how to identify and prevent security breaches, and can use their own training to mitigate the damage caused by such a breach.

While having security procedures and having security tools installed are critically important to preventing data security breaks, human error is by far the single most important cause of preventable cyber security breaches. Not following, understanding or bypassing security technology and protocols is the real world equivalent of leaving a businesses back door unlocked or neglecting to turn on the alarm system. According to CompTIA's IT Security Survey, human error, either alone or in combination with a technical malfunction, was blamed for three out of every four IT security breaches (approximately 74%). Security assurance continues to depend on human actions and knowledge as much, if not more so, than it does on technological advances. More than half the organizations surveyed (55.5%) reported the failure of staff to follow security procedures as the factor that contributed to most breaches caused by human error. Encouraging the proper training and certification of all relevant employees, in particular employees of small businesses, we believe is the single most important step this Subcommittee could take to protect the data controlled by small businesses.

Recommendations & Conclusion.

Based on our studies and the real world experiences of our members and certification holders, it is very clear that more needs to be done to raise IT security education, training and certification within the U.S. small business community. This segment of the American economy is almost entirely dependent for its IT enablement on VARs -- of which there are tens of thousands across the country. These VARs hold the key to reach small business, helping them improve their data security awareness and preparation. Small businesses and VARs alike, however, are struggling to find trained and certified employees, which our survey reveals is the most critical element in preventing IT security breaches.

To that end, one of the most important things Congress can do to improve IT security and prevent data breaches is to increase the pool of trained and certified IT employees. An important way to accomplish that is to enact the Technology Retraining and Investment Now Act for the 21st Century (TRAIN Act—H.R. 244), an idea we have supported federally and at the state level for the better part of a decade. The TRAIN bill will provide a tax credit for 50% of information and communications technology training program expenses. Just as the research and development tax credit helps companies make continuous investments in new product development, today a complementary human resources technology development tax credit is necessary to assure that there is a trained workforce capable of combating IT security breaches.

It is also clear to anyone familiar with small businesses in the United States that VARs must play the central role in any effort to reach out to small business in the areas of cyber security and data security. What is most needed is a government industry partnership that takes advantage of the unique access and perspective of the thousands of VARs who IT-enable small business in the U.S.

In this regard, Madam Chairwoman, last year we called on this Committee and on the Small Business Administration to create a public-private task force that would work to

identity IT security issues of small businesses. We believe it is important to focus on small businesses as a sector, as some issues are more unique to small businesses, while other issues might be less germane. This task force could include representation from SBA and DHS, would identify specific small business cyber security issues and make recommendations for resolution of such issues. Whatever the specific charge of this task force, we believe it is most important that we lay the groundwork now to maintain the security and productivity of existing small businesses, and those yet to be established.

Similarly, we have called on the Committee, the Department of Homeland Security, and the SBA to launch an aggressive education and outreach effort on data security and cyber security aimed specifically at small businesses using this nation's VARs as the key link in cyber security small business education.

We renew both of those recommendations today, Madam Chairwoman, and hope this Subcommittee will act on them.

In conclusion, I would like to again thank the Subcommittee for holding such an important hearing, and I, along with our 20,000 members, look forward to working with this Subcommittee to prevent data security breaches at small businesses.